Remarks:

In the Office Action mailed on June 28, 2007, the Examiner rejected claims 1-20. Applicants amend claims 1, 9, 14, and 17-19 herein. Claims 1-20 are pending in the application.

The Claims

Independent Claim 1 has been amended to simplify the claim structure, to more accurately show the method flow as described in the specification, and to eliminate the term "portable" to comply with the 35 USC 112, second paragraph rejection as described below. Independent Claims 9 and 14 have been amended to have a claim structure similar to Claim 1. Claims 17-19 have been amended to eliminate the term "portable" to comply with the 35 USC 112, second paragraph rejection as described below.

35 USC 112, second paragraph

Claims 1 and 17-20 were rejected under 35 USC 112, second paragraph as being indefinite. The Examiner pointed out that Claim 1 recites "a portable secure computing device" and "the secure computing device", and stated that "there is insufficient basis for this limitation in the claim" (Office Action, Page 2, Numbered Paragraph 5). Applicants infer that the Examiner means that there is insufficient antecedent basis for the latter limitation. Claim 1 has been amended to eliminate "portable". The Examiner made similar observations with respect to Claims 17-19. While these recite "the portable secure computing device", while the predicate claim (Claim 14) recites "a secure computing device". Thus, there may be an issue of insufficient antecedent basis for the limitation found in Claims 17-19. To harmonize the language used in

Claims 17-19 with Claim 14, the former have been amended to eliminate "portable" from the language. The Examiner observed that Claim 20 depends upon Claim 19 and inherits its deficiencies. Amendment of Claim 19, described above, rectifies this problem. Therefore, applicants respectfully request withdrawal of the rejections under 35 USC 112, second paragraph, and the allowance of the Claims.

35 USC 102

Claims 1-20 were rejected under 35 U.S.C. 102(b) as being anticipated by Blatherwick et al. (U.S. Patent No. 6,269,395) (hereinafter "Blatherwick"). Applicants traverse the rejection.

Anticipation under 35 U.S.C. 102(b) requires that each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference", *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

A brief summary of Blatherwick and the present patent application may assist in understanding how fundamentally different these two systems are. Applicants describe and claim "a system and method for preventing identity theft during interaction over a computer network" (page 1, lns. 10-11). The present invention protects a computer user, accessing remote sites over the network from an untrusted computer, from the risks of identity theft (gaining access to the user's personal information without authorization) perpetrated by means such as use of hardware or software keyboard loggers that may exist on the untrusted computer or simply by an intruder looking over a user's shoulder at a video screen monitor found in a public computing location, e.g., an Internet cafe. Applicants' invention involves maintaining personal

information on a separate secure computing device (hardware), such as a smart card, that is under the physical control of the user. The invention describes a method whereby the user causes the secure computing device to supply the user's personal information from the secure computing device to various network services through a user interface on the untrusted computer, but where the user never actually enters the user's personal information on the untrusted computer. Thus, keyboard loggers operating on the untrusted computer or simple snooping of activity on the video screen monitors attached thereto cannot be used to gain access to the private information.

Another way to look at the present invention is to consider it as a communications triangle having three nodes: the untrusted computer, the secure computing device, and the remote site accessed over the network. Private information is communicated directly from the secure computing device to the remote site bypassing the untrusted computer. Therefore, the protected private information is never exposed on the untrusted computer and cannot be maliciously obtained on the untrusted computer.

Blatherwick, on the other hand, relates to "a method and a computer system for providing access to services associated with different remote access points" (col. 1, lns. 9-11). The disclosure is said to describe "a CBS (computer-based system) *application*, [that] allows a user to access services provided by different service providers easily and transparently" (col. 6, lns. 39-42) (italics added).

Another way to view Blatherwick is that it describes a system and method in which communication is between two nodes of a network, namely, the CBS and a remote node. True, the remote node can be one of a set of nodes. However, the interaction is always directly between the CBS and the remote node. (Blatherwick, Abstract).

From these differences, it will be clear that Blatherwick does not teach or suggest Applicants' claimed invention.

Claims 1, 9 and 14

Claim 1 recites a method of effecting secure transactions that involves interactions over a network between three elements, viz., an "untrusted client computer (client)", a "server computer" and a "secure computing device". Accordingly, there are three distinct interactions; namely: an interaction between a client computer and a server, the secure interaction between the secure computing device and the client computer, and the direct interaction between the secure computing device and the server. Blatherwick does not teach or suggest, at least, the interaction between the secure computing device and the client and the interaction between the secure computing device and the server because Blatherwick fails to teach or suggest a system that involves a secure computing device.

The Examiner argues that Blatherwick teaches a method for effecting secure transactions over a computer network that includes an untrusted client computer with a user interface and a server computer in a manner designed to foil identity theft perpetrated from the client computer (Office Action, page 3, lines 10-16, *citing,* col. 5, lines 66 through col. 6, line 2). In that passage, Blatherwick recites "[f]urther, CBS [computer-based system] users wish to communicate with other CBSs, which are sometimes referred to as servers, depending upon their function. CBSs can communicate with each other through networks." The Examiner further argues that Blatherwick recites "connecting a secure computing device to the network" (Office Action, page 3, lines 17-18, *citing* fig. 1, ref. num. 11). Figure 1 does not refer to a third device within the computer network, but rather to the computer-based system that is the subject of the Blatherwick disclosure. In describing Figure 1, Blatherwick notes "the CBS can include a large number of different types of devices. As an example of one type of CBS, a telephone handset **11** is shown in Figure **1**" (col. 7, lines 3-5). While Blatherwick may disclose a network

with three devices: the CBS, SP1 (Service Provider 1) and SP2 (Service Provider 2) (see col. 7, lines 41-49), none of these devices server the role that the secure computing device serves in Applicants' claimed invention. Therefore, it is not surprising that Blatherwick fails to teach or suggest "operating the secure computing device to communicate a list of available services to the client computer", "establishing a secure connection from the secure computing device to the server", and "securely communicating private information from the secure computing device to the server over the secure connection."

Claim 1 recites "operating the secure computing device to communicate a list of available services to the client computer." The Examiner argues that Blatherwick's Figure 3.1 is a teaching of that element (Office Action, page 3, lines 19-20). However, Applicants respectfully disagree. As noted in Blatherwick, "each of the individual sub-figures of FIGS. 2-8 [i.e., including Figure 3.1] represents an example "window" of a CBS user interface screen or possibly the entire CBS screen" (Blatherwick, Col. 7, ll. 9-12). Thus, Figure 3.1 merely is the display of a user interface screen, not a communication of services available on the secure computing device from the secure computing device to the client computer.

Claim 1 further recites that "responsive to receiving the list of available services, using the user interface to display the list of available services to a user; [and] responsive to a selection of one available services by the user, operating the client to communicate selected services to the secure computing device." For this element, the Examiner argues that Blatherwick's Figures 3.1 and 3.2.1 provide the requisite teaching (Office Action, page 3, lines 21-24). Again, Applicants respectfully disagree. As noted above, all these figures are merely example windows on the user interface of a CBS. Thus, they cannot represent a teaching of a

communication of a selected service from the client computer back to the secure computing device.

Claim 1 further recites "establishing a secure connection from the secure computing device to the server" and "securely communicating private information from the secure computing device to the server over the secure connection" for which the Examiner argues that Blatherwick's Figure 12.1.2, ref. num. 166 and Fig. 12.1.2, ref. num. 170 provides the teaching, respectively (Office Action, page 6, lines 1-5). However, no part of Figure 12.1.2 gives any indication of describing interactions between the secure computing device and the server, or, importing the terminology from Blatherwick, between SP1 and SP2. Rather, as described in Blatherwick (beginning with col. 15, line 18), Figure 12.1.2 describes the "Initiate Connection with New Access Point Routine" in the CBS application that is the subject of the Blatherwick disclosure. As such, when the CBS user seeks to utilize the services of a second service provider (SP2) over a second available communications link, the CBS application invokes the "Initiate Connection with New Access Point Routine" to establish that connection (col. 15, lines 21-33). Blatherwick makes no explicit mention of an interaction between the service providers, SP1 and SP2, nor is such an interaction inferred, as required by Claim 1 of the present application.

Blatherwick only describes interactions between a CBS and any of a number of service providers (SP1 and SP2). There is no description of interactions between service providers, either in the sections cited by the Examiner, or in any other part of the disclosure. In a similar fashion, Applicants claim interactions between an untrusted client computer and both a server computer and a secure computing device. However, Applicants also claim additional interactions between the secure computing device and the server computer that Blatherwick does not describe.

To anticipate a claim, the reference must teach each element of the claim. As discussed hereinabove, Blatherwick fails to teach or suggest several, if not all, of the elements of Claim 1. Therefore Blatherwick does not anticipate Claim 1 and Claim 1 is patentable over Blatherwick.

Like Claim 1, Claims 9 and 14 recite interactions over a network between three distinct elements: an "untrusted client computer", a "server computer" and a "secure computing device". Again, there are three distinct interactions: client-to-server, client-to-secure computing device and secure computing device-to-server. As argued above in response to the rejection to Claim 1, Blatherwick teaches neither the claimed secure computing device nor the interaction between the secure computing device and the server are not taught or suggested by Blatherwick and Claims 9 and 14 are patentable over Blatherwick for, at least, the same reasons given in support of Claim 1.

Claims 2-8

Claims 2-8 are all dependant claims deriving from Claim 1, incorporate the limitation of Claim 1, provide further unique and non-obvious combinations, and are therefore patentable over Blatherwick for, at least, the reasons given in support of Claim 1 and by virtue of such further combinations. Additional grounds to traverse rejections of Claims 3, 5, 7, and 8 are described below.

Claim 3

Claim 3 recites "transmitting from the secure computing device to the server computer user identifying information." The Examiner argues that this is taught by Blatherwick (Office Action, page 4, lines 6-10, *citing* fig. 8.3, USER ID). However, as noted above, Figure 8.3 "represents an example "window" of a CBS user interface screen or possibly the entire CBS screen" (col. 5, lines 9-13). As such, the information supplied in

Figure 8.3 is provided by the CBS to either SP1 or SP2 and does not show communication of user identifying information between the server computer and the secure computing device as called for in Claim 3, and Blatherwick does not anticipate Claim 3 and Claim 3 is patentable over Blatherwick.

Claim 5

Claim 5 recites, "responsive to receiving the user identifying information, operating the server computer to establish an association among the user, the client and the secure computing device" which the Examiner argues is taught by Blatherwick (Office Action, page 4, lines 17-18 through page 5 lines 1-2, *citing* fig. 12.1.2, ref. no. 170). As noted above, Figure 12.1.2 relates to the "Initiate Connection with New Access Point Routine" in the CBS application, and the association illustrated in Reference Number 170 (PROVIDE USER ID, PASSWORD AND OTHER INFO FROM SCRIPT IN ACCESS POINT OBJECT TO ACCESS POINT) is between the CBS and the Access Point. It does not reveal creation of a three-way association in the server between "the user, the client and the secure computing device." As such, Blatherwick does not anticipate Claim 5 and Claim 5 is patentable over Blatherwick.

Claim 7

Claim 7 recites that "the server computer uses the sPIN for only one session". The Examiner argues that Blatherwick teaches the same (Office Action, page 5, lines 6-8, *citing* col.6, lines 10-16) and adds the conclusory statement that "the server does not store the PIN and therefore uses it for only one session" (id.). The cited section reads:

> Before one CBS communicates with another CBS, it is usually necessary for the CBSs to agree upon certain parameters or protocols, such as the rate of transfer of information (baud rate). Further, for security reasons, a CBS will often require a

> user from another CBS to supply a user ID and password to gain access to some or all of the CBS's services or resources.

This does not teach a server computer using the sPIN for only one session. Further, the statement that "the server does not store the PIN and therefore uses it for only one session" makes no sense. A password is typically provided by a user to a server, in order to authenticate the user onto the server and gain access to the resources of the server. In this situation, the server typically has a table with user IDs and associated passwords in permanent storage. The server then compares the password provided by the user with the correct password from permanent storage. The server typically does not delete the password from permanent storage upon a single use, but retains the password in the table for future use. Therefore, Blatherwick does not anticipate Claim 7 and Claim 7 is patentable over Blatherwick.

Claim 8

Claim 8 recites that the "secure computing device is a smart card. Examiner argues that Blatherwick teaches that a smart card (Office Action, page 5, lines 9-10, *citing* fig. 3.3.1). However, as noted above, "FIGS. 2-8 represents an example "window" of a CBS user interface screen" (col. 7, lines 10-11). A window in a user interface screen is not the same as secure computing device, and nowhere in Blatherwick is a smart card expressly disclosed or implied, and Claim 8 is not anticipated by Blatherwick and Claim 8 is patentable over Blatherwick.

Claims 10-13

Claims 10-13 are all dependant claims deriving from Claim 9, incorporate the limitations of Claim 9, provide further unique and non-obvious combinations, and are therefore patentable over Blatherwick for,

at least, the reasons given in support of Claim 9 and by virtue of such further combinations.

Claims 15-20

Claims 15-20 are all dependant claims deriving from Claim 14, incorporate the limitations of Claim 14, provide further unique and non-obvious combinations, and are therefore patentable over Blatherwick for, at least, the reasons given in support of Claim 14 and by virtue of such further combinations.

CONCLUSION

It is submitted that all of the claims now in the application are allowable. Applicants respectfully request consideration of the application and claims and its early allowance. If the Examiner believes that the prosecution of the application would be facilitated by a telephonic interview, Applicants invite the Examiner to contact the undersigned at the number given below.

Applicants respectfully request that a timely Notice of Allowance be issued in this application.

Respectfully submitted,

Date: September 17, 2007

/Anthony de Jong/
Anthony de Jong

Registration No. 60,244

The Jansson Firm
9501 N. Capital of Texas Hwy #202
Austin, TX 78759
512-372-8440
512-597-0639 (Fax)
tony@thejanssonfirm.com